IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA v. ASIF WILLIAM RAHMAN, Defendant	Case No. 1:24-CR-249

UNITED STATES MEMORANDUM IN AID OF MOTION FOR DETENTION

The defendant, Asif William Rahman, is accused of transmitting highly sensitive national defense information to uncleared persons through unsecure systems, resulting in its ultimate dissemination through a social media feed to foreign nationals. He is a flight risk and a danger to the community. Accordingly, the defendant should be detained pending trial. As an employee with the Central Intelligence Agency (CIA), the defendant swore an oath, received training, and signed multiple non-disclosure agreements to protect the nation's most classified secrets. He was entrusted to keep this country, and its allies, safe. But, on October 17, 2024, he abused that trust and put entire countries at risk: Rahman accessed TOP SECRET, compartmented national defense information about a foreign ally's plans against an adversary and unlawfully retained and transmitted those documents to others outside of the government—risking, by definition, exceptionally grave damage to the national security of the United States. Because of the defendant's acts, this information—still classified today—was broadcast on multiple social media platforms for the world to see. And the transmission occurred in an instant: through social media platforms and messaging apps, the information went from closely-held classified systems to the entire world at the push of a button.

Rahman knew what he had done was illegal, so he worked to avoid detection in ways that underscore he knows how to try to cover his tracks and is a serious risk of flight. In the days and weeks following his conduct, he deleted over 1.5 gigabytes of information from his classified computer workstation; he compiled and installed a host of applications and programs to fortify his mobile devices and personal computing equipment; and he booked international travel. When Rahman was arrested shortly prior to departing on this travel, the hand-written notes in his wallet included a "To do 10/22" list with items such as "contingencies," "vacation mid-Nov?," and "run." Having already broken his oath to protect national security, there is no reason to believe that Rahman would not try to "run" even if he promises this Court to appear.

In addition, after years of working in some of the most classified spaces of the CIA focused on multiple regions around the world, it is impossible to know how much classified information the defendant now possesses in his mind alone. He has shown what he is willing to do with that information: disclose it for his own motivations to the potential harm of the United States, including potentially through social media and messaging applications that transmit information instantaneously. As detailed herein, there are no conditions of release that can reasonably give the Court confidence that he will appear as required, or not present a danger to the community—here and abroad.

Procedural Background

On November 7, 2024, a Federal Grand Jury sitting in the Eastern District of Virginia, Alexandria Division, issued an indictment charging the defendant with two counts of violating the Espionage Act. Specifically, he is alleged to have had unauthorized possession of, access to, or control over documents relating to the national defense, and willfully communicated, delivered, transmitted or caused to be communicated, delivered, or transmitted, to any person not

entitled to receive it, in violation of 18 U.S.C. § 793(e).

On November 12, 2024, the Federal Bureau of Investigation (FBI) arrested the defendant. There is jurisdiction in the Eastern District of Virginia, where the defendant's last known residence was located. 18 U.S.C. § 3238 ("[A]n indictment or information may be filed in the district of the last known residence of the offender or of any one of two or more joint offenders."). And the prohibitions enumerated in Section 793 apply extraterritorially. 18 U.S.C. § 3239 ("The trial for any offense involving a violation, begun or committed upon the high seas or elsewhere out of the jurisdiction of any particular State or district, of section 793, may be in the District of Columbia or in any other district authorized by law.") (cleaned up). Also on November 12, 2024, the FBI conducted a search of the defendant's workspace and his U.S. government-leased residence.

On November 12, 2024, the FBI transported the defendant to the District of Guam. On November 14, 2024, pretrial services in the District of Guam issued a pretrial services report recommending that the defendant be detained pending trial. The government moved to detain the defendant pending trial and proffered evidence supporting its motion, and the defendant waived his opportunity to contest detention there. The court detained the defendant and issued an order directing that the defendant be transported to the Eastern District of Virginia. ECF 8.

Factual Background

TOP SECRET Classified Documents Posted Online

On October 17, 2024, at 5:59 P.M. EDT, a social media user, (Social Media Account 1) posted two highly classified United States Government documents—generally identifying certain actions, capabilities, and plans of a United States foreign allied government against a foreign adversary—on a public social media channel (the Social Media Channel). Both of the

documents clearly display "TOP SECRET" markings in classification banners at the top or sides, among many other markings limiting dissemination authority.[1] Social Media Account 1 included a public post that accompanied the documents, stating, in part:

> EXCLUSIVE: An informed source within the U.S. intelligence community has shared with us an extremely sensitive "top secret" U.S. intelligence document from the [U.S. government agency], dated October 15-16, detailing [foreign ally] preparations for an extensive strike inside [foreign adversary] . . . This classified report originates from the [U.S. government agency], part of the U.S. Department of Defense.

On October 17, 2024, at 6:18 P.M. EDT, the same two classified United States Government documents on another publicly-accessible social media platform by an account name similar to Social Media Account 1. A post accompanying the documents read:

> EXCLUSIVE: One of our sources in the U.S. intelligence community has shared with us an extremely sensitive top secret U.S. intelligence document, dated October 15-16, detailing [foreign ally] preparations for an extensive strike inside [foreign adversary].

Identification of the TOP SECRET Classified Documents and Their Source

On or about October 18, 2024, a U.S. Government Agency (USG Agency 1) identified the documents posted on social media as classified United States Government documents that were likely accessed through a particular United States Government computer application (USG

---

[1] Pursuant to Executive Order 12958 signed on April 17, 1995, as amended by Executive Order 13292 on March 25, 2003, and Executive Order 13526 on December 29, 2009, national security information is classified as "TOP SECRET," "SECRET," or "CONFIDENTIAL." Information is classified as TOP SECRET if the unauthorized disclosure of that information reasonably could be expected to cause *exceptionally grave damage* to the national security.

Pursuant to Executive Order 13526, information classified at any level can be lawfully accessed only by persons determined by an appropriate United States government official to be eligible for access to classified information, who sign an approved non-disclosure agreement, who receive a security clearance, and who have a "need to know" the classified information. Classified information can only be stored or discussed in an approved facility.

Application 1) hosted on servers located in the Eastern District of Virginia. USG Application 1 can generate classified United States Government documents in a unique Portable Document Format (PDF) file format. USG Application 1 logs each time a user generates a PDF version of a classified United States Government document with a specific Uniform Resource Locator (URL).

On October 18, 2024, USG Agency 1 identified a particular URL for the first document posted online (identified in the Indictment as "Document 1"). Document 1 is marked as classified at the TOP SECRET level, meaning that unauthorized disclosure of Document 1 could reasonably result in exceptionally grave damage to the national security. Similarly, on October 18, 2024, USG Agency 1 identified the other document posted online as an attachment to a classified United States Government document accessible through USG Application 1, with a particular URL (identified in the Indictment as "Document 2"). Document 2 is marked as classified at the TOP SECRET level, meaning that unauthorized disclosure of Document 2 could reasonably result in exceptionally grave damage to the national security.

Based upon a review of the documents posted to social media, the documents appear to be scans or photographs of Document 1 and Document 2, which appear to have been printed. A review of USG Application 1 logs revealed that only one user in the entire United States government accessed both Document 1 and Document 2 in the same format they appeared online between the time the documents were published on classified networks and the time the documents were posted on social media and also printed both of those documents: the defendant, Asif William Rahman.

Rahman's Access to Classified Information

The defendant is a United States Citizen and has worked as an employee of the CIA since

2016. As required for his employment, the defendant possessed a TOP SECRET level security clearance with the United States Government with access to Sensitive Compartmented Information (SCI).

Through his employment, the United States Government entrusted the defendant with access to sensitive government materials, including information relating to the national defense that was closely held by the government (National Defense Information) and classified documents and materials. As part of his duties, he was tasked with creating binders containing country specific, regional specific, and global information to brief high ranking U.S. government personnel.

In connection with his duties, the defendant signed a Classified Information Nondisclosure Agreement and multiple Sensitive Compartmented Information Nondisclosure Agreements, most recently on January 5, 2023. Both agreements provide, in part, that unauthorized disclosure or mishandling of classified information may violate U.S. law, including Title 18, United States Code, Section 793. The SCI Nondisclosure Agreement that the defendant signed contained, among other things, the following provision:

> I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government or Agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department of Agency or a contactor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be, or related to or derived from SCI, is considered by such department or Agency to be SCI. I further understand that I am obligated by law and regulation not to disclose any classified information or material in an authorized fashion.

After his arrest, the defendant spoke with the FBI in a voluntary, *Mirandized* interview and, among other things, stated generally that if the documents had been printed where he works, he would have been the one to do it.

Post-Transmission Claims of Impact

The day Social Media Account 1 posted the defendant's breach of highly sensitive national defense information to the world, the Social Media Channel featured multiple posts and conversations between its members, many of whom commented on the impact this particular classified information could have on the world. On October 17, one account forwarded the classified materials to the channel and commented, "If this is true, then it will be a war." Another user explained that the defendant's disclosure had revealed previously unknown capabilities:

> Some of these assets are literally unknown, and have never been disclosed, they do not exist in reality, or in public records at least. . . . Those assets are completely unknown and were not mentioned by OSINT [open source intelligence] accounts, military leaks, or the likes, thus [foreign ally] has extremely good OPSEC [operational security], and has yet undeclared weapons of some sorts that are ready for operational usage. American intelligence also confirms that [foreign ally] has, at least, nuclear-capable [] missiles.

By October 18, the Social Media Channel was taking credit for using the documents that the defendant had unlawfully disseminated to impact real-world events, with a user claiming that the publication of the documents had "prevented WW3."

Rahman's Actions After Transmission

After October 17, 2024, the defendant took a number of steps to avoid law enforcement detection. First, he engaged in a deletion campaign at his Top Secret workstation. From February 26, 2019 to October 30, 2020, the defendant accessed and downloaded thousands of highly classified intelligence reports focused on the Middle East in particular. Many of those

reports required highly compartmented access not available to just any Top Secret clearance holder in the government, but special "read ins," which the defendant was granted as a consequence of his work assignment at the time. Although those reports related to the defendant's job duties at the time, he was debriefed, or "read out," from those reporting compartments on or about October 2020. In other words, as he would have known from his training and agreements with the government, he no longer had legal access to these materials after October 2020. By October 21, 2024, however, the defendant continued to possess records in his personal folder on his Top Secret system that had titles indicating they contained the same highly classified intelligence to which he had access in 2019 and 2020. And, on that day—four days after transmitting the underlying TOP SECRET documents at issue—he deleted those files.[2] In fact, between October 23 and October 31, 2024, the defendant deleted approximately 1.5 gigabytes of data from his personal folder on a Top Secret system, again including files related to highly classified intelligence to which he previously had access in 2019 and 2020.

Second, the defendant's desk at his home included a handwritten list of applications and software outside of any government-suggested platforms—all intended to fortify Android electronic devices against interception and discovery. Those applications included not only fairly common encrypted messaging platforms, but also more unusual software used to customize and modify mobile devices including by "root access" to a phone's operating system. Based on a preliminary, partial extraction of a device found at the defendant's residence, he had downloaded and installed nearly all of his listed applications that would allow him to root his

[2] This deletion campaign came on the same day that U.S. news media outlets began to report that the FBI was conducting a criminal investigation into the disclosure, which the FBI director acknowledged publicly the next day. *See* https://abcnews.go.com/Politics/dod-fbi-investigating-suspected-major-intelligence-leak-israel-iran/story?id=114996628.

device and fortify well it beyond standard, factory protections. Based on a search of the defendant's person and residence, he also possessed a number of electronic devices, including three total phones, multiple laptops, and multiple large-capacity external hard drives—nearly all powered off and highly encrypted.

Third, when the FBI arrested the defendant and searched his person incident to arrest, the agents discovered several pages of cryptic, hand-written notes in his wallet. While a majority of the pages of notes reveal strings of numbers and letters that the government continues to analyze, some of that information included strings of digits surrounding a full sentence relating to the U.S. government's use of Minuteman missiles.

Fourth, and finally, the defendant planned international travel after his actions on October 17, 2024. In the hand-written notes from his wallet, he had included a "To do 10/22" list that included items such as "contingencies," "vacation mid-Nov?," and "run." As of November 4, 2024, he began to plan a trip to Thailand for the week of November 11, 2024. The FBI arrested him before he departed on that trip.

Resources and Previous Attempts to Emigrate from the United States

The pretrial services report prepared in the District of Guam revealed that the defendant has substantial financial resources, including access to a multi-million-dollar family trust, and the government expects that his pretrial report here will reflect the same. And although his wife and parents live in the Washington, D.C. area, he has previously attempted to emigrate from the United States. According to voluntary interviews of his family conducted by the FBI, the defendant and his wife previously attempted to secure Canadian citizenship, including applying to graduate school in Canada. Notably, according to those interviews, he concealed his desire to

emigrate from his parents until they happened upon an acceptance letter to a Canadian graduate school.

The Bail Reform Act of 1984 – 18 U.S.C. § 3142

Pursuant to 18 U.S.C. § 3142(a), when a defendant is arrested, the Court, in relevant part, shall issue an order that, pending trial, the person be (1) released on personal recognizance; (2) released on a condition or a combination of conditions; or (3) detained under subsection (e)." Detaining a defendant under Section 3142(e) requires a hearing "pursuant to the provisions of subsection (f)." *Id*. at § 3142(e). On December 5, 2024, the government moved to detain the defendant pending trial. The Court found that a detention hearing was warranted pursuant to Section 3142(f) and detained the defendant pending a hearing scheduled for December 6, 2024. ECF 11, 13.

Pursuant to Section 3142(g), the Court must consider whether there are conditions of release that will reasonably assure the appearance of the person as required and the safety of any other person and the community. "Subsection (g) sets out the factors that a judicial officer considers in its pretrial detention decision: (1) 'the nature and circumstances of the offense charged,' (2) 'the weight of the evidence against the [defendant],' (3) 'the history and characteristics of the [defendant],' and (4) 'the nature and seriousness of the danger to any person or the community that would be posed by the [defendant's] release.'" *United States v. Vane*, 117 F.4th 244, 250 (4th Cir. 2024) (quoting 18 U.S.C. § 3142(g)(1)–(4)). And Section 3142 "entitles the government to make evidentiary proffers during detention hearings." *Id*. at 252. Ultimately, the government's burden of persuasion is "to show by clear and convincing evidence that the defendant is dangerous or by a preponderance of the evidence that he's a flight risk." *Id*. at 251. "For pretrial detention to be imposed on a defendant, the lack of reasonable

assurance of either the defendant's appearance or the safety of others or the community, is sufficient; both are not required." *United States v. Stewart*, 19 F. App'x 46, 48–49 (4th Cir. 2001) (citing *United States v. Rueben*, 974 F.2d 580, 586 (5th Cir.1992)).

Argument

The enumerated factors under Section 3142(g) all weigh in favor of pretrial detention. There is clear and convincing evidence that the defendant poses a danger to the community, and there is a preponderance of evidence that he could flee and therefore fail to appear at future court proceedings.

First, the nature and circumstances of the offenses charged and, relatedly, the nature and seriousness of the defendant's danger posed to others make it clear the defendant should be detained. The law establishes that disclosing TOP SECRET material definitionally risks *exceptionally grave danger* to national security. And these documents are no exception: the defendant is accused of transmitting highly classified materials related to the active plans, preparation, and capabilities of a foreign ally to attack a foreign adversary. This is not information related to a single individual or even a single localized community; this information pertained to entire nation states and their armed forces. It is hard to overstate what other circumstances present graver risks of danger to human life than unilaterally deciding to transmitting information related to plans for kinetic military action between two countries. Additionally, the defendant's actions revealed information related to the United States' possession of information related to other countries, putting this country's relationships with foreign allies at risk, further endangering the lives of others on a national scale—especially at a time of volatile turbulence in the Middle East.

Finally, the defendant's choice to transmit *these* documents opens doors for him to flee

through. A United States government agency generated the highly classified documents on or about October 16, 2024, and within 36 hours, the defendant accessed, printed and unlawfully transmitted them. This speaks to both the defendant's potential antagonistic feelings toward the United States and his fervent desire to spread this information to others. *Cf. United States v. Winner*, No. 1:17-cr-34, ECF No. 163 at 5-6 (S.D. Ga.) ("Coupled with evidence that Defendant had access to classified information during her service in the Air Force and with the NSA, particularly in light of the 'covert communications package' (discussed infra) that she had created around the time of taking the NSA position and her apparent antipathy toward the United States of America, the gravity of Defendant's alleged crime is unassailable."). Foreign adversaries will surely take note. Indeed, particular adversaries will naturally be inclined to welcome and house the defendant to access whatever other information he has retained regarding the region that he has already shown a willingness to breach his oath to protect national defense information, and his conduct indicates he will be inclined to take up that offer. The defendant therefore presents a danger to the community—both at home and abroad—and a risk of flight.

Second, the weight of the evidence against the defendant is strong, favoring of detention. As detailed above, he is the *only* government employee who both accessed and printed both documents in the format they appear in online. He retained certain cryptic information on his person about United States intercontinental ballistic missile access and other information. And he engaged in significant amounts of deletion and technical fortification of personal phones and computer systems that evidences his consciousness of guilt after the unlawful transmission charged here. The weight of this evidence and the associated likelihood that he may be convicted and one day sentenced to a significant term of imprisonment are strong motivators to flee the criminal justice system to nations that may have benefited from the defendant's actions.

Third, and finally, the history and characteristics of the defendant—including his "employment," "past conduct"—also favor detention. The defendant's past conduct in his employment with the CIA highlights just how much classified information he retains, and how little he cares about his signed agreements with the government to follow the rules. As detailed above, the defendant gained access through his employment to thousands of classified documents about the Middle East alone throughout 2020 and, by 2021, was removed from that access and "read out" of the program. By law, he no longer was authorized to access those materials. But, within days of transmission of highly sensitive national defense information on October 17, 2024, he not only still appears to have retained some of those materials on his personal workstation, but also rapidly began deleting them. Deleting 1.5 gigabytes of classified materials alone in these circumstances is sufficient to favor detention. Deleting classified materials he inappropriately retained for years after illegally transmitting others should indicate to the Court that he will treat any conditions of release with the same amount of respect.

This information, collectively, provides clear and convincing evidence that the defendant is dangerous and a preponderance of the evidence that he is a flight risk. Specifically, with regard to flight risk, it is worth emphasizing again that defendant is an individual with significant means and experience living abroad. When he feared that his crimes would be detected he booked travel plans to another foreign country and had a note in his wallet suggesting that he was contemplating whether to "run." No conditions of release can reasonably secure his appearance. And as another district court concluded under similar circumstances, "[c]lassified information cannot be retrieved or un-disclosed once it is released, so the potential of harm to national security is too great a risk to place upon the promises of this Defendant." *See Winner*, *supra*, at 13.

Conclusion

For the foregoing reasons, the United States respectfully moves to detain the defendant pending trial.

Troy A. Edwards, Jr.
N.Y. Bar No. 5453741
Anthony Rodregous
Assistant United States Attorneys
U.S. Attorney's Office, EDVA
2100 Jamieson Avenue
Alexandria, VA 22314
(703) 299-3746
Troy.edwards@usdoj.gov

Brett Reynolds
Trial Attorney
National Security Division, CES